AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) An authentication method for use in a system including a first entity [[(CARD)]] and a second entity ~~(SERVER)~~ mutually communicating by way of a network [[(NET)]], wherein said first entity is adapted to authenticate said second entity and data received from said second entity, and wherein both first and second entities store the same secret key [[(K)]], said authentication method comprising the steps of:

   [[-]] receiving by said first entity a message authenticating code [[(MAC)]] and [[other]] authentication function parameters ~~(RAND, SQN, AMF, . . .)~~, said message authenticating code [[(MAC)]] being a function of said secret key [[(K)]] and said [[other]] authentication function parameters ~~(RAND, SQN, AMF, . . .)~~;

   determining by said first entity, from a sequence number included in said authentication function parameters, whether said message authenticating code and authentication function parameters have already been received by said first entity, wherein authentication is aborted without updating a failure counter in said first entity when said sequence number indicates that said message authenticating code and authentication function parameters have already been received by said first entity;

   [[-]] computing by said first entity an expected code ~~(XMAC)~~ as a function of [[from]] said ~~other~~ authentication function parameters which have been received and [[from]] said secret key [[(K)]] stored in said first entity;

   [[-]] comparing by said first entity said message authenticating code [[(MAC)]] received and said expected code ~~(XMAC)~~; [[and]]

   [[-]] aborting authentication [[if]] when the message authenticating code [[(MAC)]] received and the expected code ~~(XMAC)~~ do not match; and

   ~~said method being characterised by the further step of:~~

[[-]] updating in said first entity said failure counter every time the message authenticating code [[(MAC)]] received and the expected code ~~(XMAC)~~ do not match upon comparison by said first entity.

2. (Currently Amended) The method according to claim 1, further comprising the step of:

[[-]] preliminary checking the failure counter by said first entity before initiating authentication.

3. (Canceled)

4. (Currently Amended) The method according to claim [[3]]1, further comprising the step of:

[[-]] resetting said failure counter to its initial value if (i) the message authenticating code [[(MAC)]] received and the expected code do match and (ii) said sequence number [[(SQN)]] indicates that said message authenticating code [[(MAC)]] and [[other]] authentication function parameters ~~(RAND, SQN, AMF, ...)~~ have not already been received by said first entity;

5. (Currently Amended) A smart card ~~(CARD)~~ adapted to authenticate a remote entity ~~(SERV)~~ and data received from it, said smart card including:

[[- a]] memory storing authentication algorithms and ~~as well as authentication and encryption keys including~~ a secret key [[(K)]] which is the same as a corresponding key stored in said remote entity;

[[-]] means for receiving from said remote entity a message authenticating code [[(MAC)]] and [[other]] authentication function parameters ~~(RAND, SQN, AMF, ...)~~;

[[-]] means for computing an expected code ~~(XMAC) from~~ as a function of said [[other]] authentication function parameters and [[from]] said secret key [[(K)]];

[[-]] means for comparing said message authenticating code [[(MAC)]] received and said expected code ~~(XMAC)~~; [[and]]

[[-]] means for aborting authentication and for updating a failure counter in said smart card if the message authenticating code [[(MAC)]] received and the expected code ~~(XMAC)~~ do not match;

means for determining, from a sequence number included in said authentication function parameters, whether said message authenticating code and authentication function parameters have already been received by said smart card and if said sequence number indicates that said message authenticating code and other parameters have already been received by said first entity, aborting authentication without updating said failure counter.

~~said smart card being characterised by further comprising:~~

~~- said failure counter adapted to store the number of abortion occurrences using a failure counter; and~~

~~- means for updating said failure counter every time the comparing means indicate that said message authenticating code (MAC) and said expected code (XMAC) do not match.~~